Telstra Cloud Sight Use case: Compliance

All you need to build, automate and scale your cloud

Compliance complexity, are you in control?

Industry regulators are mandating cloud computing standards that are relevant to their market as adoption grows.

Financial firms need to adhere to Payment Card Industry Data Security Standards (PCI DSS) to protect consumers' credit card information while healthcare professionals face similar standards in the healthcare industry such as the Healthcare Insurance Portability and Accountability Act (HIPAA). Meanwhile, the Centre of Internet Security (CIS) Benchmarks are a recognised global standard and best practice for securing IT systems and data against attacks.

While most of the major public cloud vendors are compliant with major industry standards and have enhanced their security capabilities, this doesn't necessarily apply to you. Their certification doesn't include your cloud resources and data hosted on their platform. It becomes your responsibility to set up and maintain the compliance of your cloud resources while maximising the benefits of cloud computing.

How does Telstra Cloud Sight help you manage compliance?

Telstra Cloud Sight manages your eligible cloud accounts by bringing together our cloud and IT expertise into an automated, modular and evolving portal that will continue to deliver new features and capabilities to help solve your cloud challenges. Based on our best practice and cloud expertise, Telstra Cloud Sight makes it easy for you to create a compliant public cloud environment through cloud account blueprints and dashboards giving you a complete overview of your compliance status.

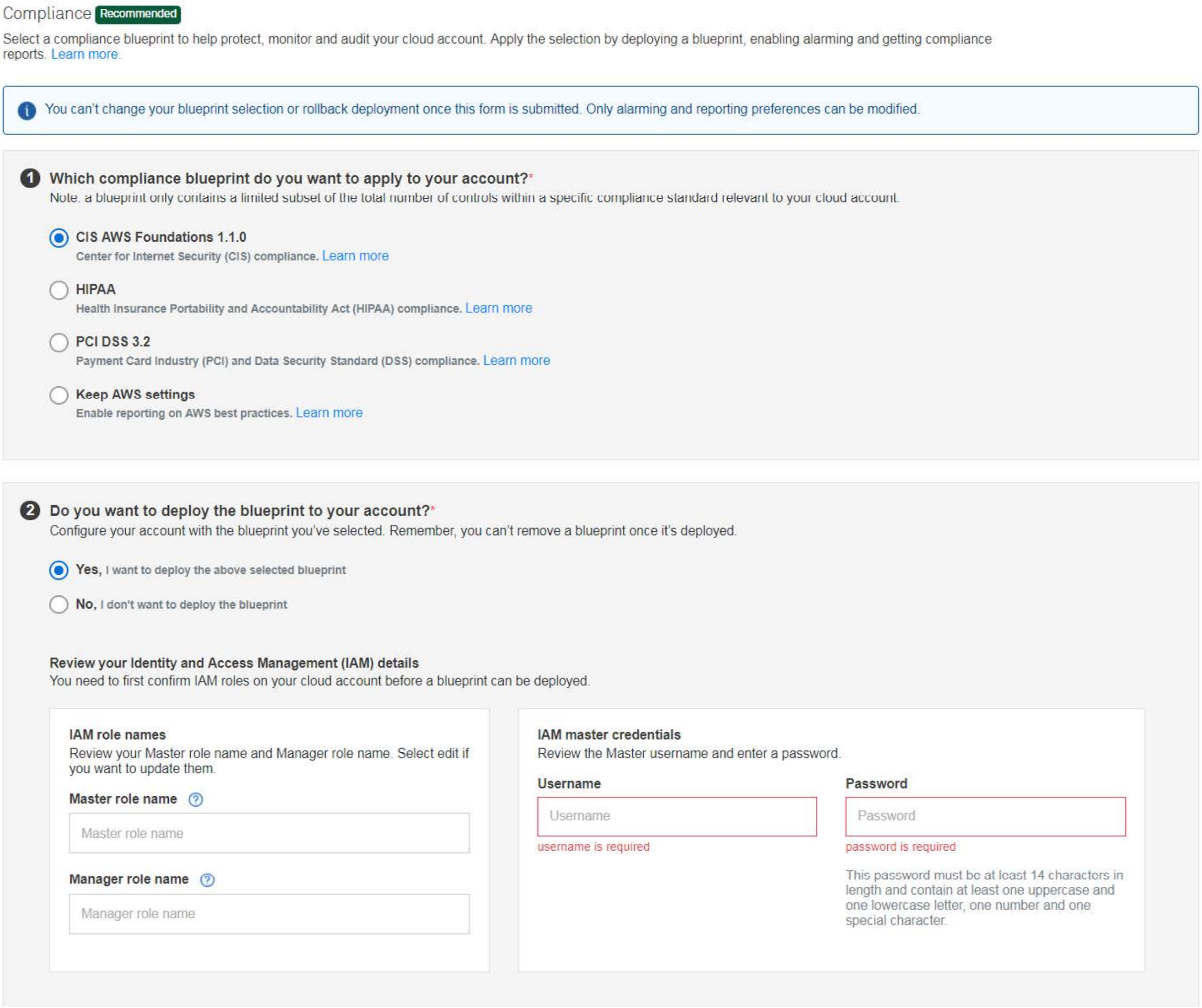
It helps you to ensure the initiation and ongoing monitoring of compliance of your public cloud accounts. This is achieved in three ways.

How it works

1. Set up your cloud accounts

New accounts

Setting up a new account with a compliance blueprint within your public cloud is easy with Telstra Cloud Sight. Telstra's long-term experience in working with compliance standards in the cloud and across multiple industries has been translated into an automated tool which will build your cloud accounts from a selectable set of blueprints.



Compliance Recommended

Select a compliance blueprint to help protect, monitor and audit your cloud account. Apply the selection by deploying a blueprint, enabling alarming and getting compliance reports. Learn more.

ⓘ You can't change your blueprint selection or rollback deployment once this form is submitted. Only alarming and reporting preferences can be modified.

1 **Which compliance blueprint do you want to apply to your account?***
Note: a blueprint only contains a limited subset of the total number of controls within a specific compliance standard relevant to your cloud account.

● **CIS AWS Foundations 1.1.0**
Center for Internet Security (CIS) compliance. Learn more

○ **HIPAA**
Health Insurance Portability and Accountability Act (HIPAA) compliance. Learn more

○ **PCI DSS 3.2**
Payment Card Industry (PCI) and Data Security Standard (DSS) compliance. Learn more

○ **Keep AWS settings**
Enable reporting on AWS best practices. Learn more

2 **Do you want to deploy the blueprint to your account?***
Configure your account with the blueprint you've selected. Remember, you can't remove a blueprint once it's deployed.

● **Yes,** I want to deploy the above selected blueprint

○ **No,** I don't want to deploy the blueprint

Review your Identity and Access Management (IAM) details
You need to first confirm IAM roles on your cloud account before a blueprint can be deployed.

IAM role names
Review your Master role name and Manager role name. Select edit if you want to update them.

Master role name ?
Master role name

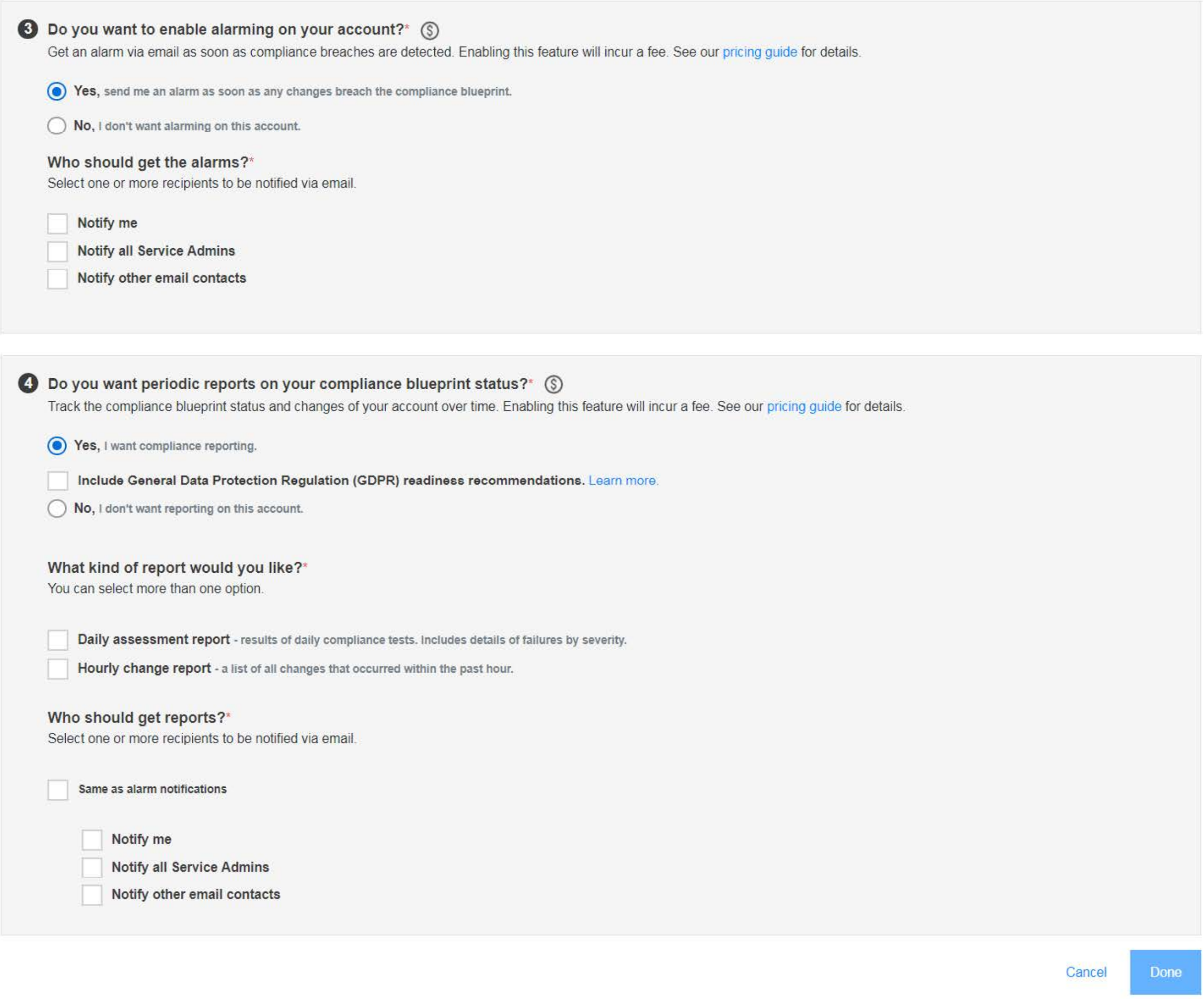
Manager role name ?
Manager role name

IAM master credentials
Review the Master username and enter a password.

Username
Username
username is required

Password
Password
password is required

This password must be at least 14 characters in length and contain at least one uppercase and one lowercase letter, one number and one special character.



3 Do you want to enable alarming on your account?* $

Get an alarm via email as soon as compliance breaches are detected. Enabling this feature will incur a fee. See our pricing guide for details.

● **Yes,** send me an alarm as soon as any changes breach the compliance blueprint.

○ **No,** I don't want alarming on this account.

Who should get the alarms?*

Select one or more recipients to be notified via email.

□ **Notify me**

□ **Notify all Service Admins**

□ **Notify other email contacts**

4 Do you want periodic reports on your compliance blueprint status?* $

Track the compliance blueprint status and changes of your account over time. Enabling this feature will incur a fee. See our pricing guide for details.

● **Yes,** I want compliance reporting.

□ **Include General Data Protection Regulation (GDPR) readiness recommendations.** Learn more.

○ **No,** I don't want reporting on this account.

What kind of report would you like?*

You can select more than one option.

□ **Daily assessment report** - results of daily compliance tests. Includes details of failures by severity.

□ **Hourly change report** - a list of all changes that occurred within the past hour.

Who should get reports?*

Select one or more recipients to be notified via email.

□ **Same as alarm notifications**

□ **Notify me**

□ **Notify all Service Admins**

□ **Notify other email contacts**

The blueprint contains a select subset of controls within the industry standard relevant to your cloud account. The blueprint simplifies the time consuming and complex work needed to develop scripts and introduce security compliance into these accounts. Choose from one of the industry standards so that the accounts are built to comply with the blueprint from the start and minimise your business risk.

List of common industry standards	List of supported Public Clouds
Centre for Internet Security (CIS) Benchmarks	Amazon Web Services
Healthcare Insurance Portability and Accountability Act (HIPAA)	Microsoft Azure (Coming soon)
Payment Card Industry Data Security Standards (PCI DSS)	

2. Enable compliance notifications

Compliance notification

There may be some actions performed on your cloud account that causes it to not be in compliance with your blueprint. When this happens, you will want to be notified at the earliest instance so that you can address the issue. The platform can be configured to send an alarm and notify you as soon as any actions that are not in compliance to the blueprints are detected.

3. Monitor your cloud accounts

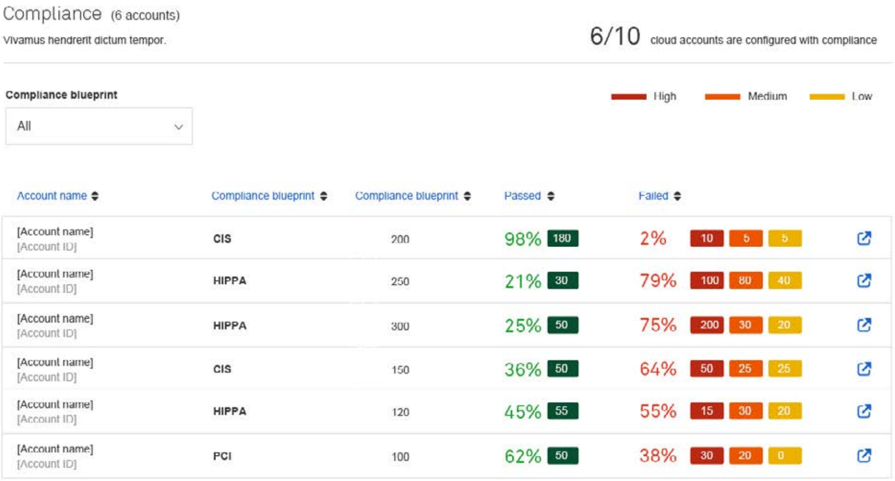
Monitoring & analytics dashboard

Monitoring is a requirement for almost all compliance frameworks. It serves to protect the implementation of the standard and offers important forensic and audit information.

Telstra Cloud Sight also offers you reporting, delivered in dashboards and email pdf format. This reporting provides a percentage score of compliance with remediation recommendations to improve this compliance score. It also gives you a historical (to day 1 of using Telstra Cloud Sight) view which is handy in audit situations.

Compliance monitoring and reporting can be implemented on accounts built through Telstra Cloud Sight and imported accounts.

The platform provides actionable intelligence for administrators, users and stakeholders of the tenancy and accounts. This allows you to make informed decisions on your risk profile in the cloud and manage your environment effectively.



Compliance (6 accounts)

Vivamus hendrerit dictum tempor.

6/10 cloud accounts are configured with compliance

Compliance blueprint

All

🟥 High 🟧 Medium 🟨 Low

Account name	Compliance blueprint	Compliance blueprint	Passed	Failed				
[Account name] [Account ID]	CIS	200	98% 180	2%	10	5	5	↗
[Account name] [Account ID]	HIPPA	250	21% 30	79%	100	80	40	↗
[Account name] [Account ID]	HIPPA	300	25% 50	75%	200	30	20	↗
[Account name] [Account ID]	CIS	150	36% 50	64%	50	25	25	↗
[Account name] [Account ID]	HIPPA	120	45% 55	55%	15	30	20	↗
[Account name] [Account ID]	PCI	100	62% 50	38%	30	20	0	↗

Telstra Cloud Sight base tier

Getting started is as simple as registering for a free Telstra Cloud Sight account and import your eligible public cloud accounts or create new accounts through the platform. Some of the compliance features are provided within the free Essential tier of Telstra Cloud Sight service. You can upgrade and subscribe to other modules subsequently.

Keeping your cloud accounts compliant with industry standards isn't the only capability of Telstra Cloud Sight. Find out how it can also help you to achieve optimisation of your cloud spend.

Essential (Mandatory base tier)
Supported Clouds: AWS
Single Sign-On Across Clouds (Console Access from the Telstra Cloud Sight platform)
Best Practice Account Deployment & Mgmt
Self Serve Cloud Cost Optimisation and Recommendations
Deploy CIS Compliant Account Architecture
Deploy PCI-DSS Compliant Account Architecture
Deploy HIPAA Compliant Account Architecture
Auto-Tagging
Resource Scheduling
Budget Controls

Contact your Telstra account representative for more details.

Australia

☎ **1300 telstra** (1300 835 787)

telstra.com/enterprise

International

☎ **Asia** +852 2983 3388 **Americas** +1 877 835 7872 **EMEA** +44 20 7965 0000 **Australia** +61 2 8202 5134

telstraglobal.com ✉ **tg_sales@team.telstra.com**